CLAIMS

What is claimed is:

1. A method for securely transferring data across an optical-switched (OS) network, comprising:

generating, at least one edge node in the OS network, security keys including an encryption key and a decryption key;

distributing, for said at least one edge node, the encryption key to at least one other edge nodes in the OS network;

encrypting, at a source edge node, data to be sent from the source edge node to a destination edge node, said data encrypted with an encryption key distributed by the destination node and received by the source node;

sending the data along a virtual lightpath between the source and destination edge nodes, the virtual lightpath spanning at least one lightpath segment; and

decrypting, at the destination edge node, the encrypted data that are sent, said encrypted data being decrypted with the decryption key generated by the destination node.

2. The method of claim 1, wherein the OS network comprises an optical burst-switched (OBS) network.

3. The method of claim 2, wherein the OBS network comprises a photonic burst-switched (PBS) network.

4. The method of claim 2, wherein the PBS network comprises a wavelength-division multiplexed (WDM) PBS network.

5. The method of claim 1, wherein the security keys are generated and distributed by:

generating a respective asymmetric key pair including an encryption and decryption key at each edge node in the OS network; and

for each edge node,

distributing the encryption key it generated to each of the other edge nodes.

6. The method of claim 1, wherein the encryption key comprises a public key and the decryption key comprises a private key, and wherein security keys are distributed by:

for at least one edge node;

receiving a digital certificate at a receiving edge node, the digital certificate containing a public key corresponding to a private key generated by a generating edge node, wherein the public key is to be used to encrypt data send from the receiving edge node to the generating edge node.

7. The method of claim 6, further comprising:

generating a self-signed digital certificate at the generating edge node; and

sending the digital certificate to the receiving edge node.

8. The method of claim 6, further comprising:

generating security data including the public key at the generating edge node;

sending the security data to a certificate authority, the certificate authority to issue an authenticated digital certificate containing the public key; and

receiving the authenticated digital certificate at the receiving edge node.

9. The method of claim 8, further comprising:

generating a respective set of security data at each edge node; and

sending the respective set of security data from each edge node to the certificate authority.

10. The method of claim 1, further comprising:

employing a trusted platform module (TPM) to generate an asymmetric key pair comprising the encryption key and the decryption key.

11. The method of claim 10, further comprising:

employing the TPM to securely store the decryption key in a manner by which it cannot be accessed by an unauthorized agent.

12. The method of claim 11, wherein the decryption key is securing stored by performing operations including:

dynamically generating a security key with the TPM;

encrypting one of a decryption key or a digital certificate containing a decryption key using the security key;

measuring an integrity metric corresponding to a platform configuration;

storing the integrity metric in a platform configuration register (PCR)

sealing the security key against the TPM using a TPM_Seal command referencing the PCR.

13. The method of claim 1, further comprising:

employing a trusted platform module (TPM) accessible to edge node that receives an encryption key to securely store the encryption key in a manner by which it cannot be accessed by an unauthorized agent.

14. The method of claim 1, further comprising sending encryption keys to said at least one other edge node using a communication channel that is external to the OS network to distribute the security keys.

15. The method of claim 1, further comprising sending encryption keys to said at least one other edge node using an out-of-band channel of the OS network to distribute the security keys.

16. The method of claim 15, further comprising sending security data via a control burst for the OS network, the security data including one or more security keys or containing information from which one or more security keys can be derived.

17. The method of claim 1, further comprising sending information to each edge node identifying at least one of an encryption algorithm and decryption algorithm to be employed to encrypt and/or decrypt the data via the security keys.

18. The method of claim 17, further comprising sending encryption and/or decryption code to an edge node, the encryption and/or decryption code to be executed to perform encryption and/or decryption operations.

19. A method for securely transferring data across an optical-switched (OS) network, comprising:

performing one of dynamically generating or selecting an encryption and decryption key at a source edge node in the OS network;

building a control burst, the control burst containing information to reserve network resources to form a virtual lightpath between the source edge node and a destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath

segment, the control burst further including security data comprising one of the decryption key or data from which the decryption key can be derived;

sending the control burst to the destination edge node;

encrypting, at a source edge node, data to be sent from the source edge node to a destination edge node, said data encrypted with the encryption key;

sending the encrypted data along the virtual lightpath between the source and destination edge nodes during the timeslot for which the virtual lightpath is reserved, and

decrypting, at the destination edge node, the encrypted data that are sent, said encrypted data being decrypted with a decryption key comprising one of the decryption key include with the security data sent via the control burst or a decryption key derived from the security data.

20. The method of claim 19, wherein the OS network comprises an optical burst-switched (OBS) network.

21. The method of claim 20, wherein the OBS network comprises a photonic burst-switched (PBS) network.

22. The method of claim 20, wherein the PBS network comprises a wavelength-division multiplexed (WDM) PBS network.

23. The method of claim 19, further comprising:

dynamically generating the encryption and decryption keys using a trusted platform module located at the source edge node.

24. The method of claim 23, wherein the encryption and decryption keys comprises a single symmetric key.

25. The method of claim 23, wherein the encryption and decryption keys comprises an asymmetric key pair.

26. The method of claim 19, further comprising:

time-bounding the decryption key so the decryption key will expire after a pre-defined timeframe; and

determining if the decryption key has expired prior to enabling the data to be decrypted at the destination edge node, wherein decryption is not allowed if the decryption key has expired.

27. The method of claim 19, wherein the security data sent via the control burst further includes information identifying an encryption algorithm to be employed to encrypt the data sent to the destination node.

28. A machine-readable medium to provide instructions, which when executed by a processor in a source edge node of an optical switched (OS) network cause the source edge node to perform operations including:

encrypting data to be sent to a destination edge node using an encryption key;

generating a control burst, the control burst containing information to reserve network resources to form a virtual lightpath between the source edge node and the destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath segment, the control burst further including security data comprising one of a decryption key or data from which the decryption key can be derived;

sending the control burst to the destination edge node; and

sending one or more data bursts containing the data that are encrypted to a first hop along the virtual lightpath during the scheduled timeslot.

29. The machine-readable medium of claim 28, wherein execution of the instructions further perform the operation of generating one of a symmetric session key or an asymmetric session key pair, the session key or key pair including the encryption key and the decryption key.

30. The machine-readable medium of claim 28, wherein execution of the instructions performs the further operation of sending a command to a trusted platform module (TPM) to generate a symmetric session key or an asymmetric session key pair, the session key or key pair including the encryption key and the decryption key.

31. The machine-readable medium of claim 28, wherein execution of the instructions performs the further operation of selecting a symmetric session key or an asymmetric session key pair for a set of security keys which may be accessed by the source edge node.

32. The machine-readable medium of claim 28, wherein execution of the instructions performs the further operation of embedding information in the control burst identifying said one or more data bursts to be sent from the edge node to the destination edge node will be encrypted.

33. The machine-readable medium of claim 28, wherein the security data include one of information identifying an encryption algorithm used to encrypt the data or executable code that may be used to decrypt the certificate.

34. A system comprising:

at least one processor;

memory communicatively-coupled to said at least one processor;

an encryption component;

a trusted platform module (TPM), communicatively-coupled to said at least one processor;

an optical interface; and

a storage device in which instructions are stored, said instructions to perform operations when executed by said at least one processor, including:

commanding the TPM to generate one of a symmetric session key or an asymmetric session key pair, the session key or key pair including an encryption key and a decryption key.

invoking the encryption component to encrypt, using the encryption key, data to be sent to a destination edge node operatively linked in communication to the system via a photonic burst-switched (PBS) network, the system to operate as a source edge node;

generating a control burst, the control burst containing information to reserve PBS network resources to form a virtual lightpath between the source edge node and the destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath segment, the control burst further including security data comprising one of the decryption key or data from which the decryption key can be derived;

sending the control burst to a first hop along the virtual lightpath, the first hop comprising one of a switching node or the destination edge node; and

sending one or more data bursts containing the data that are encrypted to a first hop along the virtual lightpath during the scheduled timeslot.

35. The system of claim 34, wherein said at least one processor includes a network processor.

36. The system of claim 34, wherein said at least one processor includes an ingress network processor and an egress network processor.

37. The system of claim 34, wherein the encryption component comprises a hardware device programmed to perform encryption operations.

38. The system of claim 34, wherein the encryption component is embodied as a software module comprising a plurality of instructions to effectuate encryption operations when executed on a processor.

39. The system of claim 34, further comprising a decryption component configured to decrypt data received from the PBS network.

40. The system of claim 39, wherein the decryption component comprises a hardware device programmed to perform decryption operations.

41. The system of claim 39, wherein the decryption component is embodied as a software module comprising a plurality of instructions to effectuate decryption operations when executed on a processor.

42. The system of claim 39, wherein the decryption component is used to determine if a time-bound decryption key has expired prior to enabling the data to be decrypted, wherein decryption is not allowed if the decryption key has expired

43. The system of claim 34, wherein execution of the instructions by said at least one processor further performs the operation of embedding information in the control burst

identifying said one or more data bursts to be sent from the edge node to the destination edge node will be encrypted.

44. The system of claim 34, wherein execution of the instructions by said at least one processor further performs the operation of time-bounding the decryption key such that the encryption key will expired after a pre-determined timeframe.